



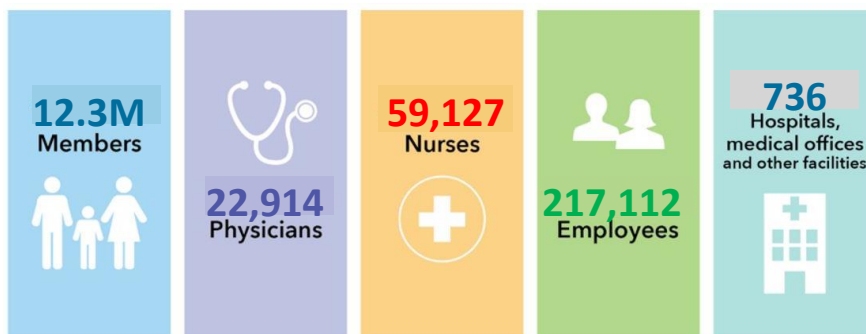
Protecting Our Patients: What Healthcare Organizations Need to Know about Cybersecurity

Eric Liederman, MD, MPH


National Leader, Privacy, Security and IT Infrastructure
The Permanente Federation

Director of Medical Informatics
The Permanente Medical Group

About Kaiser Permanente



Agenda

- Learn who is after you – and why
 - Understand common attack methods and tools
 - Review good security practices
 - Discuss joint security governance to balance privacy and security risks with patient care quality and safety
 - Consider enabling technologies such as Multi-Factor Authentication
-
- 
-

Hacked?



“There are two types of companies:
those that have been hacked,
and those who don't know they have
been hacked.”

John T. Chambers



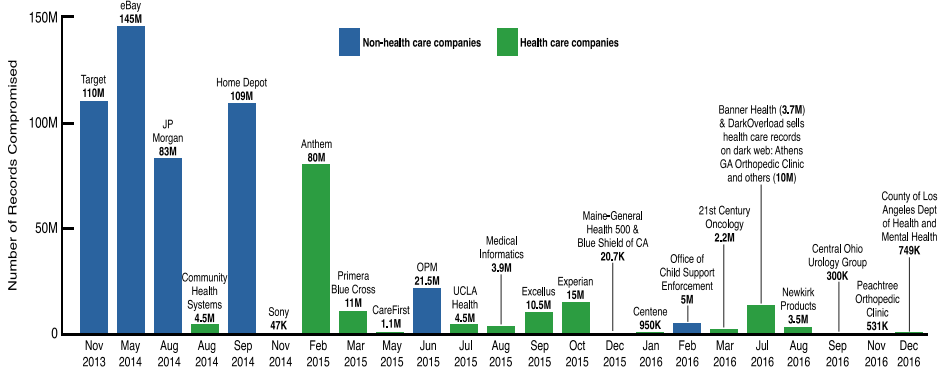
“Denial Is Not Just a River in Egypt.”

Herb Cain, David Crosby, Al Franken



Health Care: Top Target For Attackers

Snapshot of Corporate Data Breaches, 2013 - 2016



2017 Data Breaches

<p>February 2017 Emory Healthcare</p> <p>Ransomware attack; 79,930 patient records breached</p>	<p>March 2017 Urology Austin</p> <p>Ransomware attack; 279,663 patients records breached</p>	<p>May 2017 WannaCry</p> <p>Ransomware attack; 300,000+ computers infected in over 150 countries 16 UK NHS hospitals infected</p>	<p>June 2017 NotPetya</p> <p>Wipeware attack on Ukraine Spilled to many countries Merck, Nuance, 3 US hospitals infected</p>
---	--	--	---

2019 US Ransomware Impacts

363% Increase in ransomware attacks on business targets 2018 to 2019

491 Healthcare providers impacted Q1-Q3 2019

68 State & county entities impacted Q1-Q3 2019

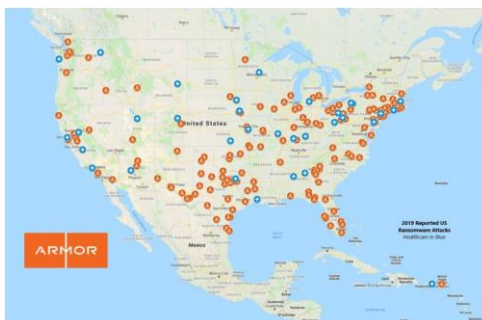
1000+ U.S. education institutions impacted Q1-Q3 2019

In 1 week in October, 4 healthcare organizations were targeted:

- 3 in Alabama
- 1 in California

Causing hospitals to:

- Redirect ambulances and ask patients to choose other hospitals
- Limit operations to existing patients and "critical new patients"
- Transferring patients from the ED



Map of YTD 2019 Reported U.S. Ransomware Attacks

Sources:
 Gibson Research Center: Security Now 10-08-19
 Bleeping Computer & Malwarebytes: US Accounts for more than half of World's ransomware attacks
 EmsiSoft: State of Ransomware in the U.S. 2019 Report Q1-Q3
 Gartner: How to Respond to the 2019 Threat Landscape

Can Breaches Kill Patients?

DOI: 10.1111/1475-6773.13203

RESEARCH ARTICLE

HSR Health Services Research

Data breach remediation efforts and their implications for hospital quality

Sung J. Choi PhD¹ | M. Eric Johnson PhD² | Christoph U. Lehmann MD³

Findings:

- Hospital time to EKG increased 2.7 minutes
- 30 day MI mortality increased 0.36 percentage points = 36 additional deaths for every 10,000 MIs

Cyber Attacks on the Health Care Industry

Cyber attackers have increased interest in targeting the health care industry, primarily due to the increasing value of protected health information.

	<u>CREDIT CARD</u>	<u>MEDICAL RECORD</u>
Estimate Value to a Criminal (per record)*	\$5 to \$15	Up to \$1000
	Short term value (single use)	Long term value (multiple uses: extortion, medical fraud, identity theft, etc..)
	Newer technologies (e.g., Chip and Pin) are making it more difficult to steal	Lagging technology is making theft easier to buy and steal – and driving the cost down

*SOURCE: Flashpoint, Dark Web Monitoring Agent, Federal Bureau of Investigation




Cybersecurity Threat Actors

	CYBER CRIME AS A SERVICE	ORGANIZED CRIME
Motive	Financially motivated, paid % of profit	Financially motivated
Characteristics	<p>Allows others to rent infrastructure for attacks: botnets, phishing tools, and vulnerability scanning of targets</p>	<p>Aim to collect ransom, personal data, including medical records, credit cards and social security numbers</p> <p>Typically have an industry focus</p> <p>Efficient, profit-focused quick attacks with high return on investment</p> <p>Increasing sophistication using denial of service ransomware</p>




Cybersecurity Threat Actors

	STATE-SPONSORED	HACKTIVISTS
Motive	Research, espionage and sensitive proprietary information	Motivated by social justice causes to seek confidential information to defame or damage an enterprise
Characteristics	<p>Highly-skilled and highly-persistent groups with unlimited resources</p> <p>Employ sophisticated and previously unknown methods (e.g., custom malware, wipeware)</p> <p>Pursue and achieve specific objectives</p> <p>Maintain a low profile to cover their tracks and remain in the network for months, if not years</p>	<p>Unstructured coalitions of individuals that come together based on common cause</p> <p>Rely on social engineering techniques</p> <p>Employ less sophisticated attack methods due to resource limitations</p> <p>Engage armies of infected computers available in the dark web</p>

Threat Vectors

 Social Engineering	Exploiting human nature	Email phishing, spear phishing and whaling; telephone and in person fraudulent representations
 Internet Surfing	Malware-laced Internet pages, links & downloads	“Drive-by” and hidden malware
 Credential Theft	Exploiting stolen user IDs & passwords	Elevated access accounts (system and database administrators, report writers) present greatest risk

Threat Vectors

 Network	Disrupt network traffic, or breach network	Movement to the cloud expands paths attackers can take, and Denial of Service attacks are challenging to prevent
 Software bugs	Software bugs, and unpatched systems	Provide breach entry points. Requires ongoing work to keep versions up to date and to apply patches across complex enterprises
 Configuration errors	Systems with configuration errors	Requires constant testing and assessment of applications and infrastructure. Biomedical devices are a special challenge

Social Engineering Threats

▪ Phishing campaigns

- Mass emails from “your bank”
- Targeted emails from “your boss” (spear phishing)
- Senior executive targeting – a “subpoena” (whaling)
- “Angler phishing” is a new tactic where criminals register fake social media accounts that masquerade as customer support accounts
 - They monitor real support accounts for irate customer messages and then quickly jump in to send messages back to those users, loaded with malicious links



▪ Imposter domains

- Appear to be legitimate websites

▪ Phone calls

- From “the Help Desk” or “Microsoft” telling you your computer has been infected and they need to remote in to fix it.

Phishing Tips

Errors and lack of detail

Be wary of emails with spelling or grammatical errors. Mass phishing emails won't address you by name; some will address you by your email address.

Sender name spoofing

Click on the sender name to see the actual email address. Is it right?

Check links

Before clicking a link in email, hover over it with your cursor and look at the bottom of your email window. You'll see destination. Does it look right?

Suspicious-looking attachments

Look at email attachment extensions to verify they are what they should be. File types of high-risk attachments include: .exe, .scr, .zip, .com, .bat.

Test your team

Periodically test with fake phishing emails. Provide positive reinforcement (when they are reported) and negative reinforcement, when links are clicked).

Privacy and Security Tips

Watch out for malicious software

Malware can disrupt the operations of your computer. If you suspect you have malware on your system, stop what you're doing, disconnect from the network and report it immediately.

Smart passwords

Don't reuse passwords. The first thing attackers will do is to try any passwords they've discovered from sites they've breached or that they've purchased on the Dark Web because they know that people frequently reuse passwords.

Don't routinely expire passwords – it just forces people to write them down on paper and in unencrypted files.

A-HED

The Man Who Wrote Those Password Rules Has a New Tip: N3v\$r M1^d!

Bill Burr's 2003 report recommended using numbers, obscure characters and capital letters and updating regularly—he regrets the error

SOURCE: Wall Street Journal, 8/7/17, page 1

Privacy and Security Tips

Protect laptops, tablets, and smartphones

Treat your mobile device or laptop like the valuable resource it is. Don't leave it unattended in insecure locations. Encrypt all devices, so they are useless if stolen.

Keep up to date with patches and antivirus

Create a software and operating system patching process and stick to it. Patches fix security vulnerabilities that are rapidly exploited by hackers. Ensure all computers have up to date antivirus running at all times.

Manage your vendors

Ensure every vendor or outside entity which handles and/or stores your Protected Health Information (PHI) has signed a Business Associates Agreement. Ask them about their patching and antivirus protections. Biomedical vendors may try to hide behind FDA 510k. The FDA's guidance: "The agency typically does not need to review or approve medical device software changes made for cybersecurity reasons"

SOURCE: <https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm189111.htm>

Multi-factor Authentication: Additional Layer of Protection

With hackers increasingly targeting healthcare, usernames and passwords may no longer be enough. A userid and password alone can allow a hacker into your system

Multi-factor authentication (MFA) requires something else to access systems (especially from outside your corporate network):

At least two of the following

- Something you know: password
- Something you have: a badge or token
- Something you are: fingerprint



MFA done right should enable work and patient care “wherever and whenever”

Build a Collaborative Governance Process

Connect Cybersecurity and clinical experts to minimize patient care and security risks

- Cybersecurity experts know how to protect against IT threats
- Clinical and operational leaders know what it takes to provide safe, high quality healthcare

Bring them together, with the aim of reducing the aggregate level of risk: security risks and patient care risks:

- Working group of key clinical and security experts
 - Structured decision venues
 - Senior executive oversight of process
-

Summary

- Healthcare is full of soft targets with money – you have a bullseye on your back
 - Keep abreast of the news – know who is after you, your money and your data
 - Develop and maintain knowledge of attack methods – and/or work with or hire someone who will
 - Educate – and test – your workforce regularly
 - Create joint discussion and decision governance
 - Push back when security proposals, policies and initiatives threaten patient care quality and safety
 - Implement enabling technologies that allow your people to get their work done, on site and at home, securely and easily
-

Paranoia

Success breeds complacency. Complacency breeds failure. Only the paranoid survive.

[Andy Grove](#)

Strange how paranoia can link up with reality now and then.

[Philip K. Dick](#)

There is no such thing as paranoia. Your worst fears can come true at any moment.

[Hunter S. Thompson](#)

Questions?

Eric.Liederman@kp.org
